UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	Criminal No. 09-10243-MLW
RYAN HARRIS	)	

GOVERNMENT'S TRIAL BRIEF

On May 18, 2011, a grand jury returned a 11-count superseding indictment charging Ryan Harris with one count of conspiracy to commit wire fraud, in violation of 18 U.S.C. § 371, and 10 counts of substantive wire fraud, as well as aiding and abetting others in the commission of wire fraud, in violation of 18 U.S.C. §§ 1343, 2. In this trial brief, the government will summarize the evidence it expects to present at trial, and it will analyze the legal issues, both substantive and evidentiary, that it anticipates might arise during trial.

I. HARRIS'S CABLE MODEM HACKING SCHEME

Over the course of six years, from 2003-2009, defendant Ryan Harris, through his $1 million commercial enterprise, TCNiSO, purposefully designed, manufactured, and distributed a series of self-styled "cable modem hacking" products and services that were intended to, and in fact did, help his users steal cable internet service from their local Internet Service Providers ("ISPs"). He helped two types of users steal service: users who were not subscribers of any internet service, and users who were subscribers but typically paid for the slowest (and therefore cheapest) level of service. With Harris's help, non-subscribers obtained internet service without paying any fees at all (i.e., they

engaged in "theft of service"), and bare-bones subscribers obtained much faster internet service without paying the required premiums (i.e., they engaged in what Harris called "uncapping").

Harris's "cable modem hacking" products and services had two key functionalities: a "packet sniffer" (which he dubbed "CoaxThief") and a MAC address/configuration file changer.[1] Through his "packet sniffer," Harris helped his users surreptitiously intercept (or "sniff") internet traffic so that the users obtained the MAC addresses and configuration files of nearby modems. Through his MAC address/configuration file changer, Harris helped his users change their modem's MAC addresses to MAC addresses belonging to legitimate, paying (or premium) subscribers and change their configuration file to one that allowed the user faster, premium internet service. In essence, Harris helped his users disguise themselves as legitimate, paying (or premium) subscribers and defraud ISPs into providing them with free or faster internet service.

But Harris did far more than just design, develop, and sell his cable modem hacking tools. He also provided ongoing, valuable assistance to ensure that his users were successful in defrauding ISPs. For example, he set up and operated an online bartering platform for his users to trade or acquire stolen MAC addresses and

[1] A cable modem is a device that connects a computer to the coaxial cable wires that provide cable internet access to that computer. Each modem has a MAC address, which, like a serial number, is a theoretically unique identifier that manufacturers hard-code into the modems at the factory. ISPs use a modem's MAC address to determine if it belongs to a legitimate, paying subscriber. If the ISP recognizes the MAC address, the ISP then electronically sends a "configuration file" to the modem. The configuration file determines the speed and other parameters of the subscriber's internet service. ISPs typically charge premiums for faster internet service.

configuration files.[2] Harris also set up and operated an online user feedback forum, on which he elicited from his users information about ISPs' efforts to detect and block his products from their networks. Harris would then design new work-arounds to defeat the ISPs' detection and blocking techniques in what was a continual game of "cat and mouse" with the ISPs. He also offered instruction manuals and online and video tutorials about how to use his products.

II. TCNiSO Insiders and Massachusetts Users

The superseding indictment references several TCNiSO insiders and Massachusetts users by their initials. The two TCNiSO insiders who worked for Harris are Craig Phillips, of San Diego, California, and Isabella Lindquist, of Louisville, Kentucky. The four Massachusetts residents who acquired and successfully used Harris's cable modem hacking products and services to steal internet access from their ISPs in Massachusetts are Nathan Hanshaw, Lasky Genao, Jose Larosa, and William Madeira. All six will be witnesses at trial.

Phillips pled guilty to an information charging him with one count of computer-related fraud. He is awaiting sentencing, having had his case transferred to the Southern District of California, pursuant to Fed. R. Crim. P. 20. Nathan Hanshaw, who was a juvenile at the time of his conviction, pled guilty in a juvenile proceeding in front of Judge Saylor. He pled to an information charging him with committing a variety of hacking crimes, including his cable modem hacking activities. He completed his 11-

[2] ISPs typically will not allow two users in the same neighborhood to share the same MAC address; either one or both users will get knocked offline. Harris's users, therefore, could not successfully use MAC addresses that they sniffed and instead had to trade them for MAC addresses of users in another neighborhood.

month sentence in a juvenile detention center. Hanshaw, now an adult, is currently in custody for violating the terms of his supervised release.

The government also initially charged Harris's now defunct company, TCNiSO, as a defendant. On December 14, 2011, the Court granted the government's motion to voluntarily dismiss the charges against the defunct corporate defendant.

III. OVERVIEW OF THE SUPERSEDING INDICTMENT

Count one alleges that Harris conspired with the two TCNiSO insiders, the four Massachusetts users, and others, to commit wire fraud. Counts two through eleven allege that Harris committed, and aided and abetted the four Massachusetts users in committing, substantive wire fraud. Specifically, counts two through five relate to wire transmissions involving Nathan Hanshaw (two wires relate to instances in which Hanshaw accessed the internet from Massachusetts to download TCNiSO's products, and two wires relate to instances in which he successfully used TCNiSO's products to access the internet without paying). Counts six through eleven relate to the three other Massachusetts users (for each user, one wire stems from the user's accessing the internet to purchase TCNiSO's products and one stems from the user's successful use of TCNiSO's products to access the internet without paying).

IV. THE EVIDENCE

A. WITNESSES

The government anticipates calling between 10 and 15 witnesses. They fall into five basic categories: (1) TCNiSO insiders; (2) Massachusetts users; (3) ISP and modem manufacturer employees; (4) law enforcement agents; and (5) records custodians (if stipulations cannot be obtained).

1. TCNISO Insiders

a. Craig Phillips

Phillips will testify at trial, pursuant to the cooperation provision in his plea agreement. The government expects that he will testify that he was an officer of TCNiSO from approximately 2003 to 2007, and he was also a longtime personal friend and onetime roommate of Harris's. He will testify that he helped Harris run TCNiSO, first while he and Harris were living in Arizona and then out of their shared apartment in San Diego. Phillips will describe the roles that Harris, Lindquist, and he played in running the company, as well as give an overview of the different products and services that TCNiSO offered. He'll describe the ongoing customer support that Harris provided, including issuing product updates to combat ISPs' blocking techniques and operating the online forums, where users traded MAC addresses and configuration files and discussed techniques for successfully stealing internet access.

Phillips is expected to testify that Harris showed him how to use the various TCNiSO products to steal free, uncapped internet access. He'll testify that, both before and while they were roommates, he saw Harris using TCNiSO products to obtain free, uncapped internet access. He will add that Harris used these products in part to transfer large video and music files at higher speeds without paying. The government believes that the testimony about Harris's use of the TCNiSO products is direct evidence of Harris's knowledge that these products were used for theft of service. But in the event that the defendant were to take the position that this testimony is evidence of "other crimes," the government is providing this notice that it would then offer the testimony under Fed. R. Evid. 404(b).

The government expects Phillips to state that he knew that the entire TCNiSO business was designed with the purpose of helping people defraud ISPs into providing free and faster internet service. Phillips will testify that he personally intended to help others defraud their local ISPs, that he believed that Harris's and his conduct was illegal, and that he was afraid of getting caught. The government expects that Phillips will testify that he repeatedly discussed with Harris the fact that their users were stealing internet access with their help and that they also discussed Phillips's fears of getting caught. Phillips will testify that Harris often told him that they would become "rich and famous" through TCNiSO and would be able to buy a large house with a pool with their proceeds. He will also testify that Harris frequently said that he hated the cable companies.

The government also expects that Phillips will refute Harris's anticipated defense that he designed the products as, and intended them to be used as, diagnostic tools. Phillips will testify that the sole intended use of TCNiSO's products and services was to steal free and faster internet service. He will state that the products had no other commercially viable legitimate use and that they were neither designed nor used as diagnostic or educational tools.

Phillips will describe Harris as paranoid and will testify about some of the efforts that Harris undertook to hide his involvement in the business operation. Phillips will testify that, for example, Harris insisted that Phillips's parents' address go on many of the corporate and business documents.

Through Phillips, the government will seek to introduce online chat communications that Harris had with Phillips himself and with various other unindicted co-conspirators, including Hanshaw. Phillips copied these chat logs when he left

TCNiSO and can therefore authenticate them. These chat logs are discussed in further detail below.

b. Isabella Lindquist

Lindquist, another TCNiSO insider, was granted letter immunity in this matter, and the government will ask the Court to grant her court-ordered immunity before her testimony at trial. She will testify that she was the primary software coder for TCNiSO from approximately 2002 through 2008. Lindquist will corroborate much of Phillips's testimony. She will describe how Harris initially reached out to her online and asked her to write software code for him. She'll describe the roles that Harris, Phillips, and she played in operating the company. She'll also describe in more detail the various products and services that TCNiSO designed and offered. She'll testify about her role in devising new products, new updates and new features. She'll state that Harris told her about forum posts in which TCNiSO customers complained about ISPs' detection and blocking techniques and that Harris then directed her to devise work-arounds to defeat the ISPs' techniques.

Lindquist will testify that she was in regular online and telephone communication with Harris during that period. Like Phillips, we anticipate that she will testify that she and Harris discussed the fact that their users were stealing internet access with their help. She will also corroborate Phillips's testimony that Harris told her that they would become wealthy together building TCNiSO. She'll also refute Harris's claim that the products were designed as diagnostic tools and state that the products had no commercially viable legitimate use.

Lindquist, like Phillips, will testify that she had numerous online communications with Hanshaw (whom she also knew only by his online nickname, "DShocker") and that Hanshaw was a long-time user of TCNiSO's products. She will testify that Hanshaw was a TCNiSO "groupie" who regularly provided technical help to other users of TCNiSO's products. Lindquist will also testify that Harris had numerous communications with Hanshaw as well.

Through Lindquist, the government will seek to introduce online chat communications that Harris had with her. These chat logs are discussed in more detail below.

Neither Phillips nor Lindquist has any criminal history.

2. Massachusetts users

Nathan Hanshaw will describe his long-time use of TCNiSO's products to steal internet access as well as his role in providing other users help in using the products. He will also testify about his direct communications with Harris, Phillips, and Lindquist. Through Hanshaw, the government will seek to introduce logs of online chat communications that he had with Harris.

As noted above, Hanshaw recently violated the terms of his supervised release, after he was arrested for attempting to break into a car. At the subsequent modification hearing, the Court ordered Hanshaw to serve three months in a community correction center/halfway house. Hanshaw fled the facility a few days after he began serving that sentence. He was arrested in early January and is currently in custody, pending a January 19, 2012 final revocation hearing.

The three other Massachusetts users will offer largely similar testimony: each purchased TCNiSO's cable modem hacking products online from, and acquired stolen MAC addresses and/or configuration files from, the TCNiSO website. They then successfully used the products and MAC addresses to steal internet access from their Massachusetts-based ISP. Through one of the users, Jose Larosa, the government will seek to introduce the computer disk he received from TCNiSO, which contains the Sigma software program. Larosa will also testify that he bought thousands of dollars worth of products from TCNiSO for his family and friends.

3. ISP and Modem Manufacturer Employees

The government will call Christopher Kohler from Motorola, a major manufacturer of cable modems, and Benjamin Brodfuehrer from Charter Communications, a major ISP in Massachusetts and around the country. Both companies are, in at least some respects, victims of Harris's crimes. Motorola makes the modems that Harris's products were designed to hack. Charter was the cable ISP from which Hanshaw, and many other TCNiSO customers, stole internet service. Kohler and Brodfuehrer will educate the jury about cable modems, cable internet access, and the way that Harris's products worked. Because portions of both Kohler's and Brodfuehrer's testimony will likely qualify as expert testimony under Fed. R. Evid. 702, the government has already provided Harris with expert disclosures for each witness.

Christopher Kohler from Motorola will provide the modem manufacturer's perspective. He'll describe cable internet service generally, Motorola's cable modems, and how cable modems work to provide internet service. He will explain what MAC addresses are and how cable companies use them to identify paying subscribers. He will

describe how, when manufacturing modems and encoding MAC addresses onto them, Motorola takes extreme measures to ensure that their MAC addresses cannot be changed. Kohler will describe his familiarity with TCNiSO's cable modem hacking products and will describe how they worked to steal free and faster internet access. He will testify that he personally tested TCNiSO products and confirmed that they in fact facilitated theft of service and uncapping. Kohler will testify that the TCNiSO products have no commercially viable use as a diagnostic tool. He'll testify that TCNiSO was by far the biggest player in the marketplace and that he received numerous complaints from many ISPs about Sigma and other TCNiSO products being used to clone Motorola's modems.

Through Kohler, the government intends to introduce several summary diagrams that describe generally how cable internet access is provided and how cable modem hacking works.

Brodfuehrer will provide the ISPs' perspective. He'll describe configuration files and explain how they determine a subscriber's internet speed. He will describe bandwidth limits and the costs that ISPs incur when they have to provide additional bandwidth to a neighborhood. He will describe "tiered" service, where ISPs charge higher fees for providing more bandwidth to a user.

Brodfuehrer will testify about theft of service and uncapping generally and will testify about his familiarity with TCNiSO's products. He will testify that he tested TCNiSO products and will explain how they allowed users to clone legitimate subscribers' MAC addresses and configuration files in order to facilitate theft of service and uncapping. He'll also testify about how users typically cannot use MAC addresses from their neighborhood to steal service.

Brodfuehrer will describe several techniques that Charter and other ISPs employed to try to detect and block TCNiSO's products from their network. He'll also describe subsequent TCNiSO product updates that defeated Charter's detection and blocking techniques. He will testify that the TCNiSO products have no commercially viable use as a diagnostic tool.

Brodfuehrer will also describe the scope of the financial injury that Charter suffered as a result of users using TCNiSO products on its network, both in terms of lost subscriber revenues and time and money Charter spent trying to detect and block cloned modems. He'll testify that TCNiSO was the "market leader" and that it accounted for the largest portion of cloned modems on Charter's network.

Through Brodfuehrer, the government will seek to introduce video clips and screen shots that show, step-by-step, how a TCNiSO product works.

4. Law Enforcement Agents

The government plans to call at least two law enforcement witnesses: FBI Special Agent Timothy Russell and IRS Special Agent Jason Ryan. SA Russell will testify that, during the course of his investigation, he reviewed the forums on the TCNiSO website.[3] He will also testify about a search warrant that the FBI served on GoDaddy, the webhosting company that hosted the TCNiSO website and e-mail, and will describe some of the documents obtained from that search. SA Russell will also testify about his on-line undercover purchase of TCNiSO's products and "DerEngel's" book, Hacking the Cable Modem.

[3] An online forum is akin to an online bulletin board, where users can post their own messages (called "posts"), read others' posts, and read series of back-and-forth posts on a specific topic, called a "thread."

Through SA Russell, the government intends to introduce various "threads" on the TCNiSO forums, as well as to highlight specific posts made by different users.[4] Through SA Russell, the government also intends to introduce excerpts from Harris's book. Where necessary, SA Russell will help decipher any technical jargon that appears in the posts and book excerpts in order to explain their meaning to the jury.

IRS Special Agent Jason Ryan will testify about TCNiSO's financial records. He will describe TCNiSO's gross revenues, the total number of purchasers, how much money Harris paid to Lindquist and Phillips, and how much Harris kept for his own personal use. SA Ryan will also testify about the types of customer information in TCNiSO's GoDaddy and PayPal records. He will testify that, for each purchase, these records reveal the date of purchase, and the name, screen name, and address of each purchaser.

Through SA Ryan, the government intends to introduce GoDaddy customer records that reflect each of the purchases made by the Massachusetts customers. (The government intends to seek a stipulation from the defendant to avoid the need for a GoDaddy records custodian to testify at trial).

Special Agents Russell and Ryan have served as joint case agents since before this case was indicted and both will have responsibility for coordinating travel and other logistics with trial witnesses. The government will therefore ask the Court whether both agents can be designated as representatives of the government under Fed. R. Evid. 615

[4] The easiest-to-read copy of the TCNiSO forums comes from an image of the company's website made by FBI Special Agent C.J Sperber, at SA Russell's direction. Because SA Sperber has been transferred to the FBI's Seattle office, the government will seek a stipulation to the authenticity of this image, in an effort to avoid the need to call SA Sperber as a witness.

and therefore be exempt from sequestration. While the government understands that it is traditional to have only one case agent so designated, the government suggests that allowing both case agents to be present during the proceedings would be in the interest of justice here for at least two reasons. First, doing so will facilitate witness coordination, by allowing the agents to work together to ensure that witnesses are apprised of the progress of the trial and are present and ready to testify when needed. Second, because the agents have different areas of expertise within the investigation, only by having both present in the courtroom will they "be able to assist in meeting trial surprises where the best-prepared counsel would otherwise have difficulty." Fed. R. Evid 615, Advisory Notes to 1974 Enactment. Nor would allowing both agents to be present prejudice the defendant. This is true because each agent's testimony will be distinct from the other's and from that of the other witnesses, thereby removing the possibility that this testimony will be tainted by the agent's presence in the courtroom throughout the trial.

5. Records Custodians

In the event that the defendant will not stipulate to the admissibility of the PayPal and GoDaddy records described above, the government will call records custodians from each entity.

B. EXHIBITS

1. TCNiSO Website Forum Posts

The government intends to introduce posts that users made on TCNiSO's online forums, which Harris operated and, in many cases, also moderated. These posts fall into four basic categories: (1) posts offering or seeking MAC addresses and configuration files; (2) posts describing ISPs' blocking techniques and offering or seeking help

circumventing them; (3) posts admitting that the user was trying to steal or had stolen free or faster internet access; and (4) posts expressing fears of getting caught and offering or seeking help for evading detection. In addition to specific user posts, the government also intends to introduce the names of topic headings for some of the forum threads. Dozens of these topic headings consisted of the names of ISPs, as well as references to seeking MAC addresses.

The government intends to introduce the posts and the topic headings through SA Russell, who personally reviewed the forums and oversaw the imaging of the TCNiSO website. In addition, we also intend to corroborate these specific posts and threads with the testimony of the four Massachusetts users. The government expects that these witnesses will testify that they visited the TCNiSO forums and obtained stolen MAC addresses on those forums.

The legal issues related to the posts' admissibility are discussed later in this brief.

2. Online Chats Between Harris and Others

The government intends to introduce evidence of online "chat" communications between Harris and Nathan Hanshaw, Craig Phillips, Isabella Lindquist, and other quasi-insiders/coders (who were identified by screen names such as "Lex," "MooreR," and "Mr. T"). A "chat" is an online, real time conversation between two or more parties. "Chat" software programs can be programmed to "log," or save, the communications. Harris saved many of his chats on the computer that he shared with Phillips, while they were roommates and business partners. Phillips copied some of the chat logs before leaving TCNiSO in 2007 and provided them to the government years later.

The government intends to introduce these logs through Phillips and, in some cases, through Lindquist and Hanshaw. The legal issues related to the chats' admissibility are discussed later in this brief.

3. Video Clips and Screen Shots Of TCNiSO's Products in Use

The government plans to introduce several video clips and screen shots that show, in a step-by-step fashion, what a user would typically see on his computer screen as he used TCNiSO's products. We will offer these video clips and screen shots (as well as a background explanation of what the video and screen shots demonstrate) through the Charter Communications witness, Benjamin Brodfuehrer. Brodfuehrer will testify that he acquired several TCNiSO products, loaded them onto a Charter laboratory computer, tested them to see how (and whether) they functioned, and recorded portions of this using video and screen-shot capture programs.

4. Demonstrative Chalks

The government also expects to use, with the testimony of Motorola employee Christopher Kohler, one or more chalks that depict how cable internet access is provided to a residence and how cable modem hacking works. It is expected that these chalks will contain graphic depictions of MAC addresses, cable modems, computers, configuration files, nodes, Cable Modem Termination Systems, coaxial cable and fiber cable lines. The government will not be seeking to introduce these chalks into evidence.

5. TCNiSO's Modems and Software

The government also intends to introduce several of TCNiSO's hardware and software products. Specifically, the government expects to introduce a TCNiSO modified cable modem, with the Sigma program already installed on it, through SA

Russell, who bought one as part of an undercover purchase from the TCNiSO website. The government will also offer a TCNiSO software disk through Massachusetts user Jose Larosa, who will testify that he bought it from the TCNiSO website and used it to steal internet access.

6. Excerpts from Harris's Hacking the Cable Modem Book

The government plans to introduce excerpts from Harris's book, Hacking the Cable Modem, through SA Russell, who purchased the book from the TCNiSO website.

7. Financial Records/Summary Chart

The government plans to introduce, through IRS agent Ryan, a summary chart that describes TCNiSO's financial records, principally obtained from PayPal, GoDaddy, and various financial institutions that Harris used in running his business. Special Agent Ryan will testify that he obtained, reviewed, and summarized voluminous financial records, all of which are admissible and have been available to the defense in discovery. The chart will describe TCNiSO's gross revenues, the total number of purchasers, how much money Harris paid to Lindquist and Phillips, and how much Harris kept for his personal use. The government will also offer, through SA Ryan, excerpts from the GoDaddy records documenting purchases from TCNiSO by the three Massachusetts customers who the government will call as witnesses (Hanshaw obtained TCNiSO's software without paying for it).

SA Ryan's chart summarizing the TCNiSO financial records will eliminate the need for witnesses to review with the jury the voluminous records, and will therefore "avoid needless consumption of time." Fed. R. Evid. 611(a). Federal Rule of Evidence 1006 provides, in pertinent part:

> The contents of voluminous writings . . . which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals or duplicates shall be made available for examination or copying, or both, by [the other party].

Although the underlying documents may be admitted, there is no requirement that they be. United States v. Milkiewicz, 470 F.3d 390, 396 (1st Cir. 2006).

VII. SUBSTANTIVE LEGAL ISSUES

A. Harris Can Be Convicted of Conspiracy and Wire Fraud Even if He Did Not Directly Communicate With Each User Or Know Their Identities

It is well settled that, in order to convict him of conspiracy, the government need not prove that the defendant "agreed specifically to or knew about all of the details of the crime, or knew every other co-conspirator or that he/she participated in each act of the agreement or played a major role . . . ." First Cir. Pattern Jury Instr. (Criminal) 4.03 (1998). In that vein, the First Circuit has held that a defendant need not directly communicate with his co-conspirators. See United States v. Mena-Robles, 4 F.3d 1026, 1033 (1st Cir. 1993) (affirming conspiracy conviction, holding that "the jury need not be presented with evidence showing that each coconspirator knew . . . every other coconspirator" and that a conspiracy may exist "*where there has been no direct contact among the participants*") (citations omitted, emphasis added).

Likewise, in order to convict a defendant of aiding and abetting, the government must prove "that the defendant associated himself with the venture, participated in it as something he wished to bring about, and sought by his actions to make it succeed." United States v. Medina-Roman, 376 F.3d 1, 6 (1st Cir. 2004) (citations omitted). The defendant "need not perform the underlying criminal act, be present when it is performed, or be aware of the details of its execution to be guilty of aiding and abetting." First Cir.

Pattern Jury Instr. (Criminal), 4.02 (1998). Accordingly, Harris can be convicted of conspiring with, aiding and abetting, or participating in a scheme with the Massachusetts users (and other users) even if he did not know their identities and never communicated directly with them.

Nevertheless, although not required to do so, the government intends to prove that Harris was well aware of Nathan Hanshaw's (online) identity, "DShocker," and had online communications with him. Further, Harris knew the names and addresses of his Massachusetts users, and he processed and shipped their product orders. Indeed, one of those users ordered thousands of dollars worth of products from Harris over the course of a year.

United States v. Pappathanasi, which the Court directed the parties to address, does not require otherwise. In Pappanathasi, this Court did note that the defendants did not have any direct communication with the franchisee co-conspirators. But significantly, the Court did not hold that, as a matter of law, such communication was required in order to establish the existence of a conspiracy to defraud the IRS. Pappathanasi, 383 F.Supp.2d 289, 293-294 (D. Mass. 2005). In Pappathanasi, the defendants' lack of any communication with the franchisees was more significant because there was arguably no other evidence that supported the inference that the defendants knew, let alone intended, for the IRS to be defrauded.

Here, by contrast, the government intends to rely on many other factors from which a jury can reasonably infer that Harris acted with the requisite intent, including: the core functionality of his products and the fact that they had no commercially viable legitimate use; Harris's ongoing assistance to his users, in terms of product tweaking,

bartering and user-feedback forums, and the like; Harris's own personal use of his products; his attempts to hide his identity; his communications with his TCNiSO co-conspirators, Nathan Hanshaw, and other users; his knowledge of multiple forum posts by users who stated that they were intending to steal or had already stolen internet access; his financial incentive to sell more products to satisfied customers; the market conditions surrounding his business; and his personal vendetta against cable companies.

These kinds of factors were not present in Pappathanasi, and the Court specifically noted as much. For example, the Court noted that the defendant's conduct was "widely known [and] not kept secret." Id. at 294. By contrast, here the government intends to prove that Harris was paranoid and was trying to hide his identity. Likewise, in Pappathanasi, this Court noted that the defendant's rebate program in question "also had other [legitimate] purposes," for example extending credit and providing a float. Id. at 293. By contrast, the government intends to prove that Harris's products, which he self-styled "cable modem hacking products," had no commercially viable legitimate use. He did not intend for them to be used as diagnostic tools, educational tools, or as garden variety modems, and they were not, in fact, used for those purposes.

Accordingly, here, in light of these additional factors, the absence of direct, in-depth communication between Harris and his users is not dispositive.

B. Harris Knew and Intended That Users *Would* Defraud ISPs and Steal Internet Service

The government intends to prove that Harris had the requisite criminal state of mind to convict him of conspiracy and wire fraud. In United States v. Goldberg, which the Court directed the parties to address, the First Circuit distinguished between an illegal conspiracy and joint action that is taken for lawful reasons but may have a "foreseeable

effect" that is unlawful. 105 F.3d 770, 773-74 (1st Cir. 1997). The First Circuit held that "the mere collateral effects of jointly agreed-to activity, even if generally foreseeable, are not mechanically to be treated as an object of the conspiracy." Id. at 774. To borrow from the "could" vs. "would" distinction in Pappathanasi, here, the government intends to prove *more* than that Harris provided his users with products and other help, knowing that his users *could* use them, among other possible uses, to steal internet access. Rather, the government intends to prove that Harris knew that his users *would* use his products and services to steal free and faster internet access. In short, the government intends to prove that theft of service and uncapping was far more than the "foreseeable" or "mere collateral" effects of Harris's conduct.

C. The Government Will Prove A Single, Hub-and-Spokes Conspiracy

The government will prove that Harris, TCNiSO insiders Lindquist and Phillips, and the named Massachusetts users were involved in a single, overarching conspiracy to defraud the ISPs into providing free and faster internet service. A single conspiracy of this nature, also referred to as a "hub-and-spokes" or "wheel" conspiracy, consists of an individual who has multiple illegal relationships (the hub) with other individuals (the spokes) not otherwise associated with a criminal enterprise. The First Circuit examines the "totality of the evidence" and has found three factors particularly helpful in determining if a single conspiracy exists: "(1) a common goal, (2) interdependence among the participants, and (3) overlap among the participants." United States v. Portela, 167 F.3d 687, 695 (1st Cir. 1999).

As to the "common goal" element, courts regularly give wide breadth to what may be interpreted as a common goal. Portela, 167 F.3d at 695 n. 3 (holding that goal of

selling drugs for profits satisfied "common goal" element and noting that the broad interpretation of common goals may have reduced the common objective test to "a mere matter of semantics") (internal citation omitted); United States v. Richerson, 833 F.2d 1147, 1153 (5th Cir. 1987) (noting common goals were found in a variety of broad activities, ranging from passing counterfeit currency to staging car accidents). The First Circuit has held that an incredibly broad goal, such as the intent to sell drugs, satisfies the prong. See United States v. Niemi, 579 F.3d 123, 127 (1st Cir. 2009); United States v. Mangual-Santiago, 562 F.3d 411, 421 (1st Cir. 2009); United States v. Sanchez-Badillo, 540 F.3d 24, 29 (1st Cir. 2008). Here, the common goal was for users to obtain free or faster internet service from ISPs by disguising themselves as legitimate, paying subscribers. In turn, the conspirators' goal was to profit financially -- the users by avoiding subscriber fees and Harris by earning sales revenues.

The second element of a hub-and-spokes conspiracy, the interdependence between the participants, focuses on "whether the activities of one aspect of the scheme are necessary or advantageous to the success of another aspect of the scheme." Portela, 167 F.3d at 695 (internal citation omitted). The inquiry also focuses on the state of mind of the participants. "Each individual must think the aspects of the venture interdependent, and each defendant's state of mind, and not his mere participation in some branch of the venture, is key." Id. (citations omitted). In this case, the activities of both Harris and the users were "advantageous" to the success of the scheme -- for example, the acquiring and trading of MAC addresses and configuration files among the users, the acquiring and sharing of intelligence about ISPs' detection and blocking techniques, as well as of other trouble-shooting and "how to" advice, among the users.

As a practical matter, a user's ability to successfully steal free or faster service depended on other users' shared input. For example, Harris's users typically needed more than Harris's cable modem and software; they also needed a legitimate MAC address that came from another neighborhood. Even if a user could, with CoaxThief, sniff valid MAC addresses from his own neighborhood, he generally could not use those identifiers himself to steal service. (As noted, ISPs typically will not provide service to two households sharing the same MAC address in the same neighborhood). Harris's forums played a key role in allowing users to trade stolen MAC addresses and configuration files with one another.

Furthermore, Harris's users also relied on one another to share intelligence about ISPs' detection and blocking techniques, to provide advice about how to use the products, and the like. Harris's products were frequently evolving, as he repeatedly tweaked them to overcome ISPs' detection and blocking techniques. Harris's forums played a key role in keeping his products up-to-date and functional. Not only was there interdependence among the various users, but Harris and his users were well aware of this interdependence. They clearly knew that they were part of a larger group of users, and they knew that they needed to obtain MAC addresses and configuration file from this larger group. They saw posts by users on the forums, with whole threads dedicated to trading MACs, trouble-shooting, user-feedback about ISP detection and blocking techniques, and tutorials.

Notably, the government need not show that each conspirator knew of or had contact with all other members, nor need it show that the conspirators knew all of the details of the conspiracy or participated in every act in furtherance of the conspiracy.

United States v. Stubbert, 655 F.2d 453, 456 (1st Cir. 1981) ("[A] conspirator need not be cognizant of the details of the conspiracy, including the identities of those participating in it"); see also Blumenthal v. United States, 332 U.S. 539, 557 (1947) ("the law rightly gives room for allowing the conviction of those discovered [to have participated in a conspiracy] upon showing sufficiently the essential nature of the plan and their connections with it, without requiring evidence of knowledge of all its details or of the participation of others"). "To hold otherwise would make insuperable the difficulties of discovery and proof in conspiracy cases, allowing conspirators to 'go free by their very ingenuity.'" United States v. Ramallo-Diaz, 455 F. Supp. 2d 22, 27 (D.P.R. 2006) (quoting Blumenthal, 332 U.S. at 557. n2). With this in mind, a number of cases have found a single conspiracy where the "spokes" were very loosely associated.

Blumenthal is instructive on this point. In that case, the Court held that a single conspiracy existed where appellants each had individual arrangements with an unknown central figure to sell whisky illegally, despite the fact that each "aided in selling only his part." 332 U.S. at 559. The Court reasoned that they "knew or must have known that others unknown to them were sharing in so large a project." Id. at 558. It held that, by their "separate agreements . . . they became parties to the larger common plan, joined together by their knowledge of its essential features and broad scope, though not of its exact limits, and by their common single goal." Id. at 557. See also United States v. Sureff, 15 F.3d 225, 230 (2d Cir. N.Y. 1994) (holding that a single conspiracy existed between a hub and two spokes, though the government introduced no evidence that the spokes knew each other, because each spoke "knew or had reason to know that other retailers were involved in a broad project for the importation, distribution, and retail sale

of narcotics and had reason to believe that their own benefits derived from the operation were probably dependent upon the success of the entire venture").

Here, the government need not prove that each of the identified Massachusetts users was interdependent upon the other identified user. It is enough to show, and the government intends to prove, that the users knew that they were involved in a "broad project" of stealing free or faster internet access for which they needed help from other users.

The third element, overlap among the participants, may be satisfied by "pervasive involvement of a single core conspirator, or hub character." Portela, 167 F.3d at 695. Here, Harris shines as a persistent hub among his many spokes. He not only provided the core product, he also provided key ongoing assistance, product updates, tutorials, and a user-feedback and bartering forum, on which the users were dependent to obtain free internet service. Thus, the evidence in this case will satisfy the First Circuit's standard for proving a single, overarching hub-and-spoke conspiracy.

D. Harris Can Be Convicted of Wire Fraud Even If He Did Not Personally Benefit

The First Circuit has held that, in the context of a wire fraud charge, the government need not allege, let alone prove, that the defendant personally benefited from the fraud scheme. "It is immaterial whether [the defendant] personally profited from the scheme." United States v. Silvano, 812 F.2d 754, 758-62 (1st Cir. 1987) (rejecting defendant's argument that the government did not prove that the defendant in an honest services mail fraud prosecution "in any way personally profited from his activities"). Although the honest services wire fraud landscape has changed in the wake of McNally and Skilling, this premise, which applies to classic wire fraud as well, remains intact. See

United States v. Vila, 2009 U.S. Dist. LEXIS 2729 (D. PR. 2009). In Vila, the defendant moved to dismiss wire fraud charges, arguing that "the wire fraud charges are defective because they do not allege that [the defendants] personally benefited . . . ." Id. at 9. The Court rejected this argument, reasoning that it is immaterial whether the defendant personally or directly profited from the scheme. Id.

Consistent with this principle, it is similarly well settled that a defendant can be convicted of wire fraud even when the scheme was never completed, no benefit accrued to anyone, and no loss ultimately took place. For example, in United States v. Potter, one of the authorities mentioned by this Court, the First Circuit held that the fact that one party to a wire fraud scheme might prove unwilling or unable to perform, or that the scheme never achieved its intended end, does not preclude conviction for either the substantive offense of wire fraud or for conspiracy to commit wire fraud. 463 F.3d 9, 17 (1st Cir. 2006) (affirming convictions for honest services wire fraud where defendants' contemplated monetary payments to state official's law partner were never actually made). Accord United States v. Louderman, 576 F.2d 1383, 1387 (9th Cir. 1978) (holding that that "in a prosecution under 1343 . . . the prosecution need not prove that the scheme was successful or that the intended victim suffered a loss or that the defendant secured a gain. The gist of the offense is a scheme to defraud and the use of interstate wires to further that scheme") (internal citation omitted).

Here, the government need not prove that Harris benefited at all, let alone benefited directly, when his users defrauded the ISPs into providing them with free or faster internet service. Indeed, as set forth in Potter and Louderman, Harris can be

convicted of conspiracy and wire fraud even if the government could not prove that his users succeeded in defrauding the ISPs.

Nevertheless, although it is not required to do so, the government intends to prove that the Massachusetts users were successful in defrauding their ISPs. It also intends to prove that Harris benefited indirectly from his users' success. The more successful Harris's customers were, the more products they would buy from him, the more prospective customers they would refer to his website, and the more he would profit financially. Furthermore, the government will prove that Harris benefited in an intangible way from his users' success because he was able to satisfy a long-held personal vendetta against cable companies.

VIII. EVIDENTIARY ISSUES

A. Posts on TCNISO Website Forums

1. Posts about MAC address swapping are not hearsay

As described above, the government intends to offer posts and threads by users who stated that they were seeking or offering MAC addresses and configuration files. Such posts are verbal acts rather than statements; as such, they are not hearsay. Statements that are not assertions or that have independent legal significance, such as words by contracting parties, statements giving consent, or offers, are not hearsay. United States v. Diaz, 597 F.3d 56, 64 (1st Cir. 2010). Likewise, verbal acts are not hearsay. United States v. Faulkner, 439 F.3d 1221, 1225-27 (10th Cir. 2006) (holding that statements of planning, directing, or agreement of conspiracy are verbal acts, not hearsay); United States v. Bellomo, 176 F.3d 580, 586-87 (2d Cir. 1999) (holding that

statements offered as commands, threats or rules directed toward a witness are not hearsay, so no foundation for co-conspirator statements need be established).

Even if the Court were to conclude that they are statements rather than verbal acts, these posts are not being offered for the truth of the matters asserted and are therefore not hearsay. Courts have held that out-of-court statements are admissible when offered to show their effect on the listener and not offered for the truth of the matter asserted. See, e.g., Bellomo, 176 F.3d at 586-87 (holding that declarant's statement that victim was killed because he was dealing drugs was not hearsay because it was offered for listener's state of mind, not reason for murder); United States v. Darby, 744 F.2d 1508, 1524 (11th Cir. 1984) (holding that statement that declarant knew of witness' brother's location was offered for effect on listener); United States v. Nieto, 60 F.3d 1464, 1468 (10th Cir. 1995) (holding that declarant's instructions to defendant to take car and make drugs into squares were not hearsay because introduced for effect on listener).

Here, the government will offer the posts to help show that Harris *knew* that his users were posting on his forums that they were trading MAC addresses and configuration files. In this vein, through testimony by Lindquist, Phillips, and Hanshaw, the government will show that Harris read the forums. The government intends to rely on ample other evidence to show the underlying truth that users were bartering MAC addresses and configuration files on TCNiSO's website, including through testimony of Phillips, Lindquist, Hanshaw and the other Massachusetts users.

2. User posts about stealing service and uncapping are not hearsay and in any case are co-conspirator statements

The government intends to introduce posts from users who state that they are planning to steal internet access or uncap or that they have, in fact, successfully done so. As with the MAC swapping posts, these posts are not offered for their truth; rather they are offered to show Harris's knowledge (or belief) that users were using his products and other services to steal and uncap. Furthermore, in the event that the Court determines that the posts about stealing service and uncapping are being offered for the truth of the matters asserted, they are still admissible because they are not hearsay but are instead co-conspirator statements. Fed. R. Evid. 801(d)(2)(E) provides: "A statement is not hearsay if . . . it is offered against an opposing party and was (E) a statement by the party's coconspirator during and in furtherance of the conspiracy."

Admission of a co-conspirator statement requires that four elements be satisfied by a preponderance of the evidence: 1) a conspiracy must have existed; 2) the defendant must have been a member of it; 3) the declarant must also have been a member; and 4) the declarant's statement must have been in furtherance of the conspiracy. United States v. Colón-Díaz, 521 F.3d 29, 35-36 (1st Cir. 2008); United States v. Marino, 277 F.3d 11, 25 (1st Cir. 2002). The statement need only further any conspiracy, not necessarily the one charged. United States v. Maliszewski, 161 F.3d 992, 1008 (6th Cir. 1998). Furthermore, such statements are admissible even when no conspiracy is charged. United States v. McDowell, 918 F.2d 1004, 1009 (1st Cir. 1990).

A defendant need not be aware of the details of the statement for it to be admissible against him. Marino, 277 F.3d at 25. The proponent of the evidence must show the conspiracy by evidence including "some extrinsic proof," United States v.

Sepulveda, 15 F.3d 1161, 1182 (1st Cir. 1993), and cannot rely exclusively on the statement itself. Here, the government intends to prove that the declarants are co-conspirators through the testimony of Special Agents Russell and Ryan, who will testify that the posters purchased TCNiSO products. Furthermore, the government expects that Hanshaw and Phillips will testify that they were familiar with some of the posters' online nicknames.

Courts have held that a statement is in furtherance of a conspiracy if it "tends to advance the objects of the conspiracy as opposed to thwarting its purpose." United States v. Rodriguez, 525 F.3d 85, 101 (1st Cir. 2008). "The reporting of significant events by one coconspirator to another advances the conspiracy." Sepulveda, 15 F.3d at 1180. Likewise, statements made to keep other coconspirators "abreast of the conspiracy's activities [are] in furtherance of the conspiracy." United States v. Aviles-Colón, 536 F.3d 1, 7 (1st Cir. 2008) (citing Sepulveda, 15 F.3d at 1180).

As a procedural matter, in order to conserve judicial resources, the Court should conditionally admit the statements and make its determination about the existence of the conspiracy at the close of all of the evidence. United States v. Ciampaglia, 628 F.2d 632, 638 (1st Cir. 1980); United States v. Petrozziello, 548 F.2d 20 (1st Cir. 1977). Notably, whether each user was a part of a separate conspiracy with Harris or each was part of a single hub-and-spokes conspiracy is of no moment in determining the statements' admissibility.

The posts that report that the user succeeded, or failed, in stealing access or uncapping provided information to Harris (and other users) about the efficacy of the products. Both sets of information let Harris know which ISPs were more or less

vulnerable and where to focus his tweaking efforts. These posts therefore tend to "advance the objects" of the conspiracy and constitute "reporting of significant events."

The posts about theft of service and uncapping are therefore admissible both because they are relevant to Harris's knowledge and because they are co-conspirator statements.

B. The Logs of Online Chats Are Admissible

As is mentioned above, Harris chatted on-line with several TCNISO insiders and quasi-insiders, and the government intends to introduce excerpts from these chat logs through Phillips (who copied them from TCNISO's computer and who himself communicated via chat with Harris) and through Lindquist and Hanshaw, who communicated with Harris in some of the chats.

The chat log excerpts that the government intends to offer contain one-on-one chats between Harris and the following TCNiSO insiders and quasi-insiders: Lindquist, Phillips, Hanshaw, "MooreR," "Lex," and "Mr. T." Among the topics Harris discusses in these chats are: the design and production of TCNiSO's products; that insiders and customers were using these products to steal service; that Harris's goal was to make as much money as possible as quickly as possible from TCNiSO; and that one quasi-insider ("Mr. T") was being criminally prosecuted for theft of service.

These chat log excerpts are admissible under a variety of theories. Harris's own statements in the chat logs are admissible as party admissions. Fed. R. Evid. 801(d)(2). The statements by those with whom Harris is chatting are admissible (a) to give context for Harris's statements; (b) to show Harris's knowledge and intent; and (c) as co-conspirator statements.

It is well established that courts may admit statements made by another person during a conversation with the defendant to give context to the defendant's statements. See United States v. Colon-Diaz, 521 F.3d 29, 38 (1st Cir. 2008) (holding that statements constituted reciprocal and integrated utterances and merely served to put co-conspirator's statement into perspective and make it intelligible to the jury).

Alternatively, the statements of those chatting with Harris are admissible as non-hearsay because they are not offered for their truth but rather because they are relevant to Harris's knowledge of what his products were being used for, that is, for their effect on the listener.

A third theory of admission for the statements made by the insiders and quasi-insiders with whom Harris chatted is that they are co-conspirator statements. The law of co-conspirator statements is discussed above. These chat excerpts fall within the co-conspirator exception first because Harris was communicating with co-conspirators. Lindquist and Phillips will each testify about their roles in the conspiracy to establish themselves as co-conspirators. Hanshaw will testify (and Phillips and Lindquist will corroborate) that he: was a quasi-insider; was a long-time user of the products; was in regular contact with Lindquist, Phillips, and Harris; and made frequent posts, regularly offering advice and answering other users' questions. Phillips, Lindquist, and Hanshaw will testify that MooreR, Lex, and Mr. T also were quasi-insiders, with a regular presence on the forums. They will testify that MooreR was a software coder who helped with TCNiSO's packet sniffer and MAC changer functionality, that Lex was also a software coder for TCNiSO, and that Mr. T was a friend of Harris's and a reseller of TCNiSO products.

The statements that Harris's co-conspirators make in their chats with him are admissible as co-conspirator statements because they were made in furtherance of the conspiracy. See Colón-Díaz, 521 F.3d at 35-36. Discussions about design and production of TCNiSO's products, the uses of these products to steal service, the financial success of the business, and the prosecution of one quasi-insider all constitute "[t]he reporting of significant events by one coconspirator to another" and therefore fall within the scope of the co-conspirator statement exception to the hearsay rule. Sepulveda, 15 F.3d at 1180.

Respectfully submitted,

CARMEN M. ORTIZ
United States Attorney

By: */s/ Adam Bookbinder*
Adam J. Bookbinder
Assistant U.S. Attorney
Mona Sedky
DOJ Trial Attorney

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Adam J. Bookbinder

Dated: January 13, 2012